SAFEGUARDING DATA WITH PRIVILEGED USER ACCESS CONTROLS

THE FLAW IN THE SYSTEM
Since the introduction of multi-user computer systems over 40 years ago, there has been a fundamental flaw in their security architecture. The flaw? – The concept of a Root User, Domain Administrator, System Administrator or other high level computer operator – and their data access rights. These users have always had access to every aspect of a system – software installation, system configuration, user creation, networking, resource allocation and more, as well as access to all the data associated with the system.

These accounts exist because of the need for system maintenance and management. But, as systems have become more closely interlinked and with increasing amounts of private and confidential data accessible to them, there is increased risk from privileged user accounts. Compounding this are the ways that many enterprise IT departments have traditionally done business, and the advent of new technologies and threats:

• Rights too broadly assigned – Superuser privileges are often assigned to DBAs, application developers, SysAdmins and others that don’t have a real “need” for this level of access to private and confidential data.

• Sharing of privileged accounts – Traditionally, many IT departments allowed unrestricted sharing of privileged user accounts (logins and passwords), leading to a loss of personal accountability.

• Cloud, virtualization and big data expand the threat – With each new technology layer used as part of system deployment and management new privileged user roles are created.

• Advanced Persistent Threat (APT) attacks target privileged accounts – Attackers have now found that if you want access to everything, you want to compromise privileged user accounts and their system and data access rights.

“With commercial tools, such as Vormetric, you can actually give certain people certain access without root-level privileges. You can encrypt your data in storage to set up roles of who actually gets to see the data. The admins can do their jobs, and they don’t get access to any data files.”

Robert Bigman
Former CISO

“100% of breaches involved stolen credentials.”

Mandiant – April 2013

Vormetric Data Security Solutions enables privileged users to do their jobs, and never see protected data.
WHY ORGANIZATIONS PROTECT AGAINST PRIVILEGED USERS

Organizations that need to protect data from the inherent risks of privileged users typically need to do so in order to:

- **Meet Compliance Requirements** – Segregation of roles by user type to protect specific data types such as credit card information for PCI-DSS and Personally Identifiable Information (PII) under the US HIPAA/HITECH acts.

- **Prevent Data Breaches** – Data breach laws such as US Federal and State data protection laws, the EU Data Protection Directive, South Korea’s Personal Information Protection Act (PIPA) and the UK Data Protection Act pose fines and costly notification requirements on loss of protected data.

- **Safeguarding Intellectual Property** – With government sponsored attacks a reality for manufacturers and infrastructure providers, and their primary target intellectual property (IP), organizations now need to secure data from both malicious insiders as well as from partners and contractors.

THE SOLUTION – VORMETRIC DATA SECURITY SOLUTIONS

The tasks performed by privileged users to maintain, repair and initiate systems are not optional – these roles were created in order to meet real enterprise requirements that are not going away. What's needed is to enable these users to perform their tasks, while removing their ability to view private and confidential data. Vormetric Data Security solutions are:

- **Transparent** – Vormetric Data security meets these needs with a transparent solution – enabling critical system processes to continue, without exposing data. Using protections at the file system and volume level, the solution allows the meta-data and file system structure to be seen by administrators, but reveals only encrypted data to these accounts.

- **Strong** – The Vormetric solution encrypts your data – using a policy driven approach, linked to LDAP and system accounts, that provides granular access to protected structured information (in databases) or unstructured data (in file systems) by process, user, time and other parameters. Vormetric even monitors and prevents access by tracking how users become their role. If a Root user creates a new account with data access rights, then escalates to become that account, Vormetric will still identify that account with the Root user and prevent access to cleartext data.

- **Efficient** – Vormetric Encryption is a high performance, low overhead solution, leveraging the AES NI hardware encryption built into Intel x86 processors. The result: Minimal changes to response times for operational processes.

- **Easy** – Deployments in days to weeks, not weeks to months, across physical systems, cloud, big data, and virtualized environments that are easy to manage, easy to understand.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps over 1,400 customers, including 17 of the Fortune 30 and many of the world’s most security conscious government organizations, to meet compliance requirements and protect what matters — their sensitive data — from both internal and external threats. The company’s scalable Vormetric Data Security Platform protects any file, any database and any application — anywhere it resides — with a high performance, market-leading data security platform that incorporates application transparent encryption, privileged user access controls, automation and security intelligence. For more information, please visit: [www.vormetric.com](http://www.vormetric.com).

Copyright © 2014 Vormetric, Inc. All rights reserved. Vormetric is a registered trademark of Vormetric, Inc. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Vormetric.